UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,487	08/16/2001	Edward W. Kohler JR.	12221-006001	3664

26161 7590 06/14/2006

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
ISMAIL, SHAWKI SAIF	
ART UNIT	**PAPER NUMBER**
2155	

DATE MAILED: 06/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,487	KOHLER ET AL.	
	Examiner	Art Unit	
	Shawki S. Ismail	2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

RESPONSE TO AMENDMENT

1. This communication is in response to the Amendment received on March 13, 2006.

Claims 1, 3, 4, 6, 8-12, 15-20, 22-23 and 25-31 have been amended.

Claims 1-33 are pending.

The Old rejection maintained

2. The rejection is respectfully maintained as set forth in the last Office Action mailed on December 2, 2005. Applicants' arguments with respect to claims 1-33 have been fully considered but they are not persuasive and the old rejection is maintained

Claim Rejections - 35 USC §102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

4. Claims 1-12 and 15-33 are rejected under 35 U.S.C. 102(e) as being anticipated by **Yavatkar et al.,** (Yavatkar) U.S. Patent No. **6,735,702.**

5. As to claim 1, Yavatkar teaches a method of protecting a data center against a denial of service attack, the method comprises:

sending queries to data collectors, deployed at different points in a network that carries network traffic to the data center, the data collectors collect statistical information on network packets sent over the network, the queries to request the statistical information from at least some of the data collectors (col. 3 line 65 – col. 4, line 23);

sending the statistical information from the data collectors in response to the queries (col. 3 line 65 – col. 4, line 23);

processing the statistical information to determine the source of suspicious network traffic heir sent to the data center (col. 3, lines 25-37 and col. 18, lines 32-53, agents are deployed at different areas of the network for the detection and diagnosing of various network attacks as well as for collecting statistical information on a particular node).

6. As to claim 2, Yavatkar teaches the method of claim 1 wherein the network packets from the attacker have faked, random source addresses that change with time, and sending queries further comprises:

sending queries to the data collectors for the statistical information based on victim destination address (col. 13, lines 44-53 and col. 3, line 65 – col. 4, line 23, the agents are deployed to specific areas of the network depending on the source of the attack).

7. As to claim 3, Yavatkar teaches the method of claim 1 wherein processing further comprises:

Determining, from at least in part, the collected statistical information, what data centers are involved in the attack on the victim data center (col. 8, lines 32-53, the agents determine the source of the attack and other nodes that it affected).

8. As to claim 4, Yavatkar teaches the method of claim 3 wherein determining is performed by a control center that receives the statistical information from the data collectors, and determining further comprises:

sending data to/from a gateway device that is associated with the victim data center (col. 13 line 54 – col. 14, line 17, the gateway associated with the attack is identified and measures are taken to filter the attack).

9. As to claim 5, Yavatkar teaches the method of claim 4 wherein the gateway identifies the network address of the victim, via a message to the control center (col. 13 line 54 – col. 14, line 17).

10. As to claim 6, Yavatkar teaches the method of claim 5 wherein the queries and the statistical information are sent over a redundant network that does not carry the packet traffic to deliver collected statistical information to a central control enter in response to the queries sent from the central control center (see Fig. 3).

11. As to claim 7, Yavatkar teaches the method of claim 5 wherein message indicates the type of attack (col. 3, lines 35-45 and col. 4, lines 41-61).

12. As to claim 8, Yavatkar teaches the method of claim 1 wherein a source of the attack is behind a gateway (col. 13 line 54 – col. 14, line 17)

13. As to claim 9, Yavatkar teaches the method of claim 8 wherein if a source of the attack is behind a gateway, the control center issues a request to the gateway that the

attacking system is behind to prevent the attacking traffic from attacking system from reaching the network (col. 13 line 54 – col. 14, line 17).

14. As to claim 10, Yavatkar teaches the method of claim 8 wherein if a source of the attack is behind a gateway, the gateway that the attacking system is behind selectively discards traffic that appears to be malicious traffic and that contains the victim destination address (col. 13 line 54 – col. 14, line 17).

15. As to claim 11, Yavatkar teaches the method of claim 1 wherein if source of the attack is not behind a gateway, the control center queries the data collectors to provide information about possible locations of the attacking system (col. 13 line 54 – col. 14, line 17).

16. As to claim 12, Yavatkar teaches the method of claim 1 wherein if source of the attack is not behind a gateway, the method further comprises:

contacting administrators at locations involved in the attack to have the administrators take action to filter out packets with the destination address (col. 13 line 54 – col. 14, line 17, and col. 18, line 54 – col. 19, line 6).

17. As to claim 15, Yavatkar teaches a method of protecting a victim data center against a denial of service attack, the method comprises:

receiving packets with faked, random source addresses (col. 13, lines 44-53);

receiving, from a gateway disposed near the victim data center, a notification that the victim data center is under an attack (col. 13 line 54 – col. 14, line 17, and col. 18, line 54 – col. 19, line 6);

sending queries to data collectors deployed at different points in a network that carries network traffic to the victim data center, the data collectors to sample network packets and collect statistical information on network packets sent over the network the queries being request for statistical information from data collectors that have examined network traffic with the victim destination address (col. 3, lines 25-37 and col. 18, lines 32-53); and

determining the data center or centers involved in the attack on the victim data center by analyzing collected statistical information from the data collectors (col. 18, lines 32-53).

18. As to claim 16, Yavatkar teaches the method of claim 15 further comprising:

Communicating statistical information from the control center to/from a gateway device that is disposed with the victim data center (col. 13 line 54 – col. 14, line 17).

19. As to claim 17, Yavatkar teaches the method of claim 16 wherein if a source of the attack is behind a gateway, the control center issues a request to the gateway to block the attacking traffic (col. 13 line 54 – col. 14, line 17).

20. As to claim 18, Yavatkar teaches the method of claim 17 wherein if a source of the attack is behind a gateway, the gateway selectively discards traffic that appears to be malicious traffic and that contains the victim destination address (col. 13 line 54 – col. 14, line 17).

21. As to claim 19, Yavatkar teaches the method of claim 15 wherein if a source of the attack is not behind a gateway, the method comprises:

contacting administrators at locations involved in attack to filter out packets having the destination address (col. 13 line 54 – col. 14, line 17, and col. 18, line 54 – col. 19, line 6).

22. As to claim 20, Yavatkar teaches a system to thwart denial of service attacks on a victim data center, the system comprising:

a plurality of monitors dispersed throughout a network, the monitors collecting statistical data on network traffic (col. 3, lines 25-37 and col. 18, lines 32-53);

a control center coupled to the plurality of data collectors, the control center executing a computer program product stored on a computer readable medium, comprising instructions for causing a computer to:

receive from the victim site a notification that the victim data center is under an attack (col. 13 line 54 – col. 14, line 17, and col. 18, line 54 – col. 19, line 6); and in response to receiving the notification,

send queries to data collectors to request the statistical information from the data collectors, the statistical information used to determine the source of suspicious network traffic being sent to the victim (col. 3, lines 25-37 and col. 18, lines 32-53);

a gateway device that passes network packets between the network and the victim data center, the gateway disposed to protect the victim data center, and being coupled to the control center (col. 13 line 54 – col. 14, line 17).

23. Claims 21-33 do not teach or define any new limitation beyond claims 1-20 above, therefore, they are rejected for similar reasons.

Claim Rejections - 35 USC § 103

24. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

25. Claim 13 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Yavatkar et al.,** (Yavatkar) U.S Patent No. **6,735,702** and in view of **Hill et al.,** (Hill) U.S. Patent No. **6,088,804.**

26. As to claim 13 and 14, Yavatkar teaches a method for blocking denial of service and address spoofing attacks on a network. However, Yavatkar does not explicitly teach wherein the attacks are classified into categories based on the severity that they cause to the network.

Hill teaches a system and method for adaptively responding to computer network security attacks. Hill further teaches classifying attacks based on the severity of the attack on the network (Fig. 3, col. 2; lines 53-60; col. 6, lines 9-22).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate Hill's classification of the severity of attacks into the invention of Yavatkar in order minimize the load on the computer network. Displaying attack information would help the network manager prioritize the severity of the attacks

so that it spend less time countering lesser threats and more time countering severe threats (col. 2, lines 47-53).

Response to Arguments

27. Applicant's arguments with respect to claim 1-33 have been fully considered but they are not persuasive. Applicant argues in substance that:

(A) Argument: Yavatkar does not teach that the bloodhound agents are responsive to queries for statistical information.

Response: The applicant is reminded that the claims must be given their broadest reasonable interpretation. The claim language merely recites sending queries to data collectors...to request statistical information and does not specify the type of query. Yavatkar teaches wherein on detecting an attack the watchdog agent launches various types of bloodhound agents based on the type of attack detected. Examiner is equating the launching of the various types of bloodhound agents to launching various types of queries to each bloodhound agent upon its creation based on the type of attack detected. Each bloodhound agents is designed to trace traffics from one type of attack. The gathered information is equated to the statistical information because the claim language merely recites statistical information and does not specify the type of statistical information that is collected. After gathering information (statistical information) a bloodhound agent reports to the watchdog agent automatically without having to wait for the watchdog agent to request the information because the request has been established upon the creation of the bloodhound agent and therefore a

second request is not needed. Therefore, Yavatkar creation of the bloodhound agents and gathering of the information by the agents meets the scope of the currently claimed limitations.

28. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shawki S Ismail whose telephone number is 571-272-3985. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached at 571-272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shawki Ismail
Patent Examiner
June 9, 2006

SALEH NAJJAR
SUPERVISORY PATENT EXAMINER